Best Available Copy

RECEIVED
CENTRAL FAX CENTER
AUG 20 2007

Listing of Claims:

1. (previously presented) A method for scanning network devices connected to a network, comprising:

(a) detecting connection of a first network device to the network;

(b) performing remote agentless scanning of internal files and data within the internal files on the first network device to determine internal security settings therefrom, the remote agentless scanning being performed automatically in response to detection of the first network device to thereby avoid downloading a software agent to the first network device;

(c) comparing the internal security settings determined through the remote agentless scanning with predefined security settings to determine compliance therewith; and

(d) automatically performing a remote installation of a security software program on the first network device if the internal security settings are not in compliance with the predefined network settings.

2. (original) The method of claim 1 wherein step (a) further comprises inspecting data packets communicated over the network.

3. (original) The method of claim 1 wherein the detecting step further comprises querying a database.

PAGE 5/18 * RCVD AT 8/20/2007 6:15:13 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/6 * DNIS:2738300 * CSID:801 578 6999 * DURATION (mm-ss):03-36

4. (original) The method of claim 3 further comprising continuously broadcasting pings on the network, continuously examining address resolution protocol tables, continuously monitoring event logs, transmitting a Lightweight Directory Access Protocol (LDAP) query, and transmitting a Domain Name System query.

5. (original) The method of claim 1 wherein step (b) further comprises determining at least one of whether the first network device is plugged into a wall socket, whether the first network device is connecting to the network via wireless access, and whether the first network device is connecting to the network via wireless access, and whether the first network device is connecting to the network via a Virtual Private Network.

6. (original) The method of claim 1 wherein step (b) further comprises determining a property of the first network device.

7. (previously presented) The method of claim 1 wherein step (b) further comprises determining an identity of the first network device.

8. (original) The method of claim 7 wherein the determining of the identity of the first network device further comprises at least one of querying a database where the type has been determined, examining network traffic, analyzing network behavior, probing the first network device for signature responses, attempting to log

PAGE 6/18 * RCVD AT 8/20/2007 6:15:13 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/6 * DNIS:2738300 * CSID:801 578 6999 * DURATION (mm-ss):03-26

BEST AVAILABLE COPY

into the device using a series of protocols, logging into the first network device and querying data within the device.

9. (original) The method of claim 1 wherein step (b) further comprises scanning at least one of a configuration, file, data, a software version, a patch, inventory, hardware, and a security vulnerability of the first network device.

10. (original) The method of claim 1 wherein step (b) further comprises updating at least one of a configuration, file, data, a software version, inventory, and a security vulnerability of the first network device.

11. (canceled)

12. (previously presented) The method of claim 1 wherein step (b) further comprises determining if the first network device is part of a windows domain.

13. (original) The method of claim 1 further comprising at least one of enabling the first network device to have additional access to the network, denying the first network device access to the network, notifying another about the first network device based on results of the scan, and quarantining the first network device.

PAGE 7/18 * RCVD AT 8/20/2007 6:15:13 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/6 * DNIS:2738300 * CSID:801 578 6999 * DURATION (mm-ss):03-36
BEST AVAILABLE COPY

Best Available Copy

14. (original) The method of claim 1 further comprising at least one of setting a security policy on the first network device, auditing the security policy of the first network device, ensuring compliance with a predetermined security policy, and reporting results.

15. (previously presented) An apparatus for remote agentless scanning of network devices on a network comprising:

(a) a detecting module that detects connection of a first network device to the network; and

(b) a scanning module that performs remote agentless scanning of internal files and data within the internal files on the first network device to determine internal security settings therefrom, the remote agentless scanning being performed automatically in response to the detection of the first network device to thereby avoid downloading a software agent to the first network device;

(c) comparing the internal security settings determined through the remote agentless scanning with predefined security settings to determine compliance therewith; and

(d) automatically performing a remote installation of a security software program on the first network device if the internal security settings are not in compliance with the predefined network settings.

16. (original) The apparatus of claim 15 wherein the detecting module continuously polls a database for data corresponding to newly attached network devices.

17. (original) The apparatus of claim 16 wherein the scanning module remotely scans the first network device upon detecting data corresponding to the first network device in the database.

18. (original) The apparatus of claim 15 further comprising a history database storing scan results of a scan performed by the scanning module.

19. (original) The apparatus of claim 15 wherein the scanning module can at least one of enable the first network device to have additional access to the network, deny the first network device access from the network, notify another about the first network device based on results of the scan, and quarantine the first network device.

20. (original) The apparatus of claim 15 further comprising a security policy management module for at least one of setting a security policy on the first network device, auditing the security policy of the first network device, ensuring compliance with a predetermined security policy, and reporting results.

PAGE 9/18 * RCVD AT 8/20/2007 6:15:13 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/6 * DNIS:2738300 * CSID:801 578 6999 * DURATION (mm-ss):03-36
BEST AVAILABLE COPY

21. (previously presented) A method for examining a first network device connected to a network, comprising:

(a) querying a database for data representing connection of network devices to a network;

(b) determining connection of a first network device to the network by locating data about the first network device in the database;

(c) determining properties associated with the first network device to determine the identity of the first network device;

(d) determining items to scan based on at least one of the properties; and

(e) performing remote agentless scanning of internal files and data within the internal files on the first network device to determine internal security settings therefrom, the remote agentless scanning being performed automatically in response to the determination of the connection of the first network device to the network to thereby avoid downloading a software agent to the first network device.

22. (original) The method of claim 21 wherein step (c) further comprises determining at least one of credentials associated with the first network device and type of the first network device.

23. (original) The method of claim 21 wherein step (c) further comprises at least one of querying a database where the identity has already been determined, examining network traffic, analyzing network behavior, probing the device for signature responses, and logging into the device to query data.

PAGE 10/18 * RCVD AT 8/20/2007 6:15:13 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/6 * DNIS:2738300 * CSID:801 578 6999 * DURATION (mm-ss):03-36

BEST AVAILABLE COPY

24. (original) The method of claim 21 wherein step (e) further comprises selecting a set of security policy settings to audit.

25. (original) The method of claim 21 further comprising at least one of allowing the first network device to have additional access to the network, denying access to the network, notifying another about the first network device based on results of the remote scanning, and quarantining the first network device.

26. (canceled)

27. (previously presented) The method of claim 1 wherein the scanning of internal files and data in step (b) comprises scanning a stored configuration of hardware and software on the first network device.

28. (previously presented) The method of claim 27 wherein the scanning of internal files and data in step (b) comprises scanning for incorrectly configured hardware and software.

29. (previously presented) The method of claim 1 wherein the scanning of internal files and data in step (b) comprises scanning for incorrectly configured hardware and software.

BEST AVAILABLE COPY

30. (previously presented) The method of claim 1 wherein the scanning of internal files and data in step (b) comprises scanning to determine a software version.

31. (previously presented) The method of claim 1 wherein the scanning of internal files and data in step (b) comprises scanning a software patch.

32. (previously presented) The method of claim 1 wherein the scanning of internal files and data in step (b) comprises scanning for viruses.

33. (previously presented) The apparatus of claim 15 wherein the scanning module scans a configuration of hardware and software on the first network device.

34. (previously presented) The method of claim 15 wherein the scanning module scans to determine a software version.

35. (canceled)

36. (previously presented) The method of claim 15 wherein the scanning module scans a software patch.

37. (previously presented) The apparatus of claim 15 wherein the scanning module scans for viruses.

PAGE 12/18 * RCVD AT 8/20/2007 6:15:13 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/6 * DNIS:2738300 * CSID:801 578 6999 * DURATION (mm-ss):03-36

BEST AVAILABLE COPY

38. (previously presented) The method of claim 31 wherein automatically performing a remote installation of a security software program in step (d) comprises installing a new version of the software patch.

39. (previously presented) The method of claim 1 wherein the scanning of internal files and data in step (b) comprises searching for a predetermined anti-virus software, and wherein automatically performing a remote installation of a security software program in step (d) comprises installing the predetermined anti-virus software if the predetermined anti-virus software is not found in step (b).

40. (previously presented) The method of claim 1 wherein the scanning of internal files and data in step (b) comprises determining whether firewall software is installed, and wherein automatically performing a remote installation of a security software program in step (d) comprises installing the firewall software if it is determined in step (b) that the firewall software has not yet been installed.

41. (previously presented) The method of claim 36 wherein automatically performing a remote installation of a security software program in step (d) comprises installing a new version of the software patch.

42. (previously presented) The method of claim 15 wherein the scanning of internal files and data in step (b) comprises searching for a predetermined anti-virus

PAGE 13/18 * RCVD AT 8/20/2007 6:15:13 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/6 * DNIS:2738300 * CSID:801 578 6999 * DURATION (mm-ss):03-36
BEST AVAILABLE COPY

software, and wherein automatically performing a remote installation of a security software program in step (d) comprises installing the predetermined anti-virus software if the predetermined anti-virus software is not found in step (b).

43. (previously presented) The method of claim 15 wherein the scanning of internal files and data in step (b) comprises determining whether firewall software is installed, and wherein automatically performing a remote installation of a security software program in step (d) comprises installing the firewall software if it is determined in step (b) that the firewall software has not yet been installed.

44. (previously presented) The method of claim 21 further comprising comparing the internal security settings determined through the remote agentless scanning of internal files and data with predefined security settings to determine compliance therewith.

45. (previously presented) The method of claim 21, wherein the remote agentless scanning comprises searching the first network device to determine whether anti-virus software is installed on the first network device.

46. (previously presented) The method of claim 21, wherein the remote agentless scanning comprises searching the first network device to determine whether firewall software is installed on the first network device.

PAGE 14/18 * RCVD AT 8/20/2007 6:15:13 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/6 * DNIS:2738300 * CSID:801 578 6999 * DURATION (mm-ss):03-36

BEST AVAILABLE COPY